IMPLEMENTACIÓN DE SERVICIOS IT EN ZENTYAL SERVER

Jhon Stiven Mejia Lopez
jsmejial@unadvirtual.educo
Ricardo Suarez Galvis
rsuarezga@unadvirtual.edu.co
Andres Felipe Aguilera Diaz
afaguilerad@unadvirtual.edu.co
Carolina Calero Millan
dccalerom@unadvirtual.edu.co
Andres Mauricio Rendon Ocampo
amrendon45@unadvirtual.edu.co

RESUMEN**:** *con el diplomado de profundización del sistema operativo Linux, se pudo realizar la instalación y configuración de la distribución Zentyal server en el cual se realizaron en ambientes simulados, tareas que permiten dar soluciones confiables al cliente, implementando servicios de mayor nivel IT. Dentro de las tareas realizadas se efectuaron la configuración en los diferentes módulos como son DNS Server, DHCP Server, Controlador de dominio, Proxy, Firewall, File Server, Print Server y VPN. Así mismo, se verifico el funcionamiento de cada uno de los servicios instalados.*

PALABRAS CLAVE: Linux, Zentyal, servicios, configuración.

1 INTRODUCCIÓN

En el sistema operativo Linux existen diversas herramientas que permiten cumplir con la infraestructura IT y así cubrir las necesidades de una empresa. Esto permite que la administración del sistema sea un proceso menos complejo y costoso. Una de estas herramientas es Zentyal server, la cual contiene un paquete de servicios que ayuda a la gestión de la infraestructura de la red, este fue diseñado para ser una alternativa a Windows server, contando con una interfaz gráfica amigable y sencilla de usar, la cual se puede acceder desde un navegador. Desde el panel es posible configurar servicios tales como DNS Server, DHCP Server, Controlador de dominio, Proxy, Firewall, File Server, Print Server y VPN.

2 INSTALACIÓN DEL SERVIDOR ZENTYAL

Como primer paso se debe descargar la imagen ISO de Zentyal de https://zentyal.com/community/ y montar una nueva máquina virtual. Se puede asignar para un funcionamiento mínimo y óptimo 2048MB de RAM y 80GB de memoria interna. También, antes de iniciar la instalación se deben activar dos adaptadores de red para poder simular la zona DMZ, un adaptador puente y un adaptador con red interna.

Una vez que se inicie la máquina lo primero que se debe elegir es el idioma y luego el tipo de instalación.

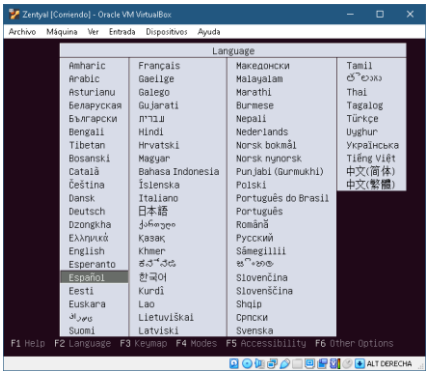

Figura 1. Selección de idioma

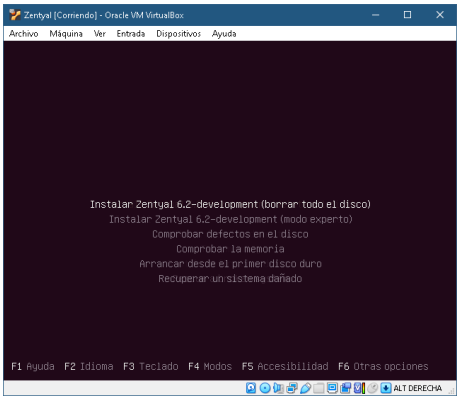

Figura 2. Instalación limpia

Elegir el país, idioma del teclado y su distribución.

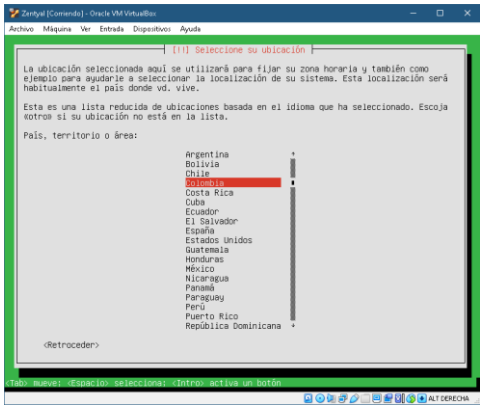

Figura 3. selección de país

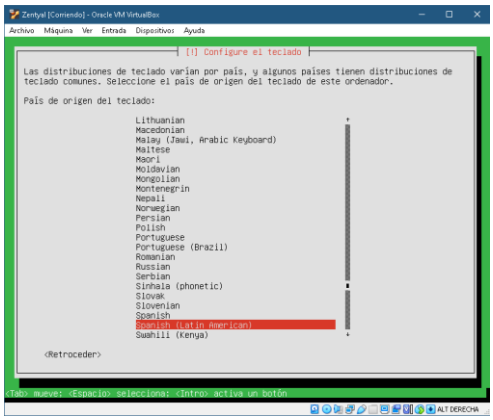

Figura 4. selección de idioma del teclado

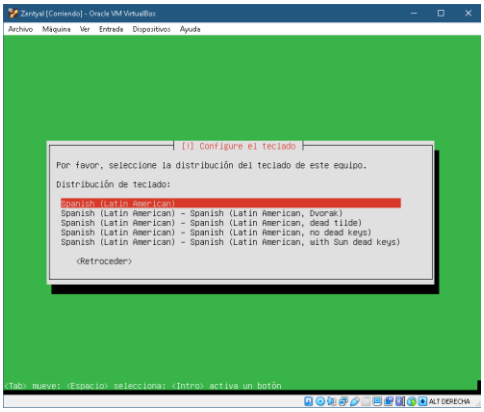

Figura 5. selección de distribución del teclado

En la configuración de red elegir la primera que es el adaptador puente.

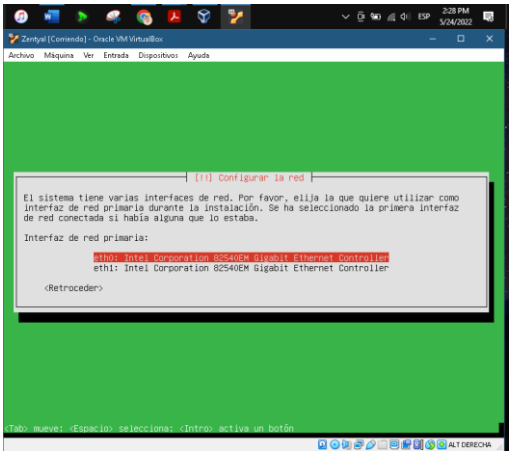

Figura 6. selección de interfaz de red

Asignar un usuario para la cuenta, nombre para la máquina y contraseña.

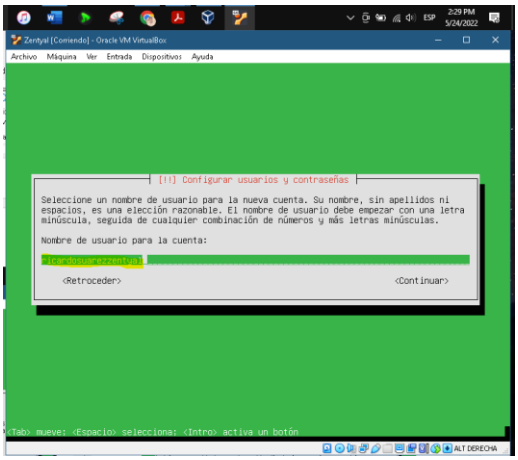

Figura 7. nombre de usuario

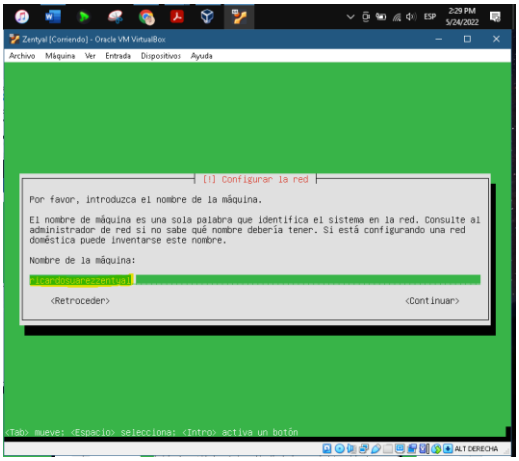

Figura 8. nombre de la máquina

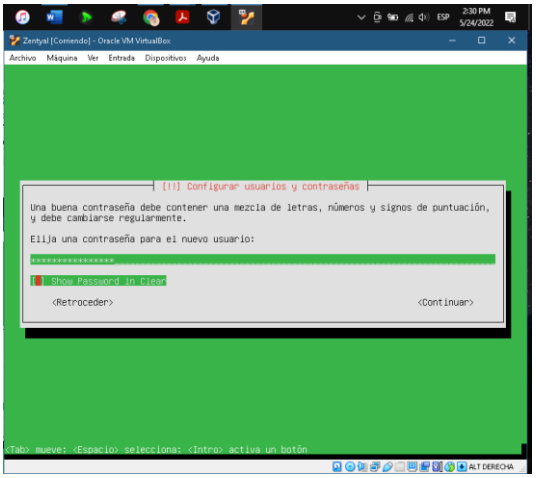

Figura 9. contraseña del usuario

El sistema detecta automáticamente la zona horaria y elegir sí es la correcta.

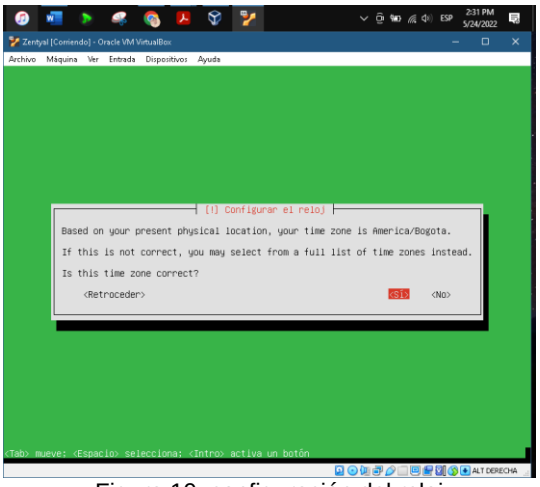

Figura 10. configuración del reloj

Cuando la instalación finaliza saldrá un aviso de que la máquina debe reiniciarse.

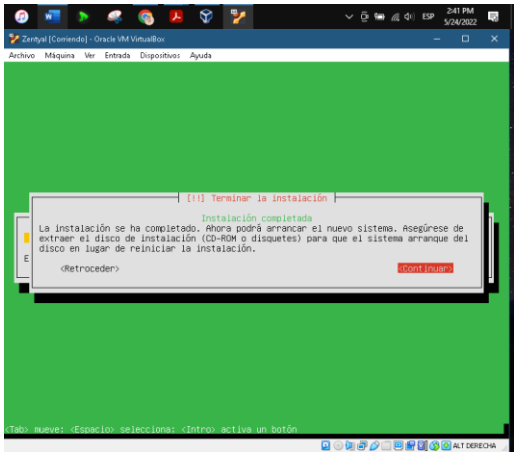

Figura 11. fin de la instalación

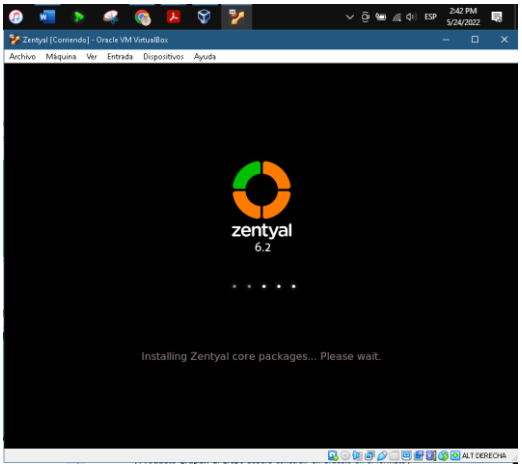

Figura 12. Inicio de Zentyal

Cuando Zentyal inicia por primera vez, automáticamente abre su navegador e ingresa a la ventana de inicio de sesión para poder iniciar la configuración de este, por lo que solo basta con avanzar e ingresar con el usuario y empezar a instalar los servicios que se necesiten.

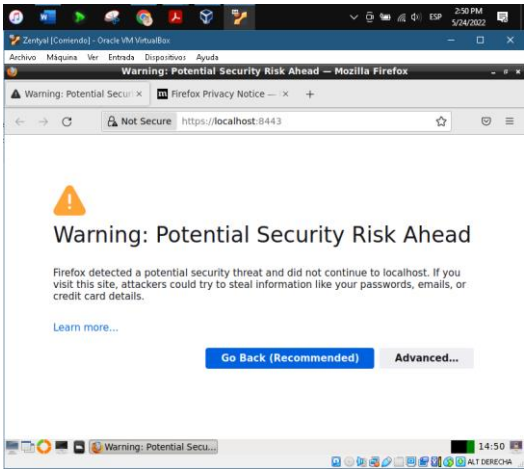

Figura 13. acceso a configuración

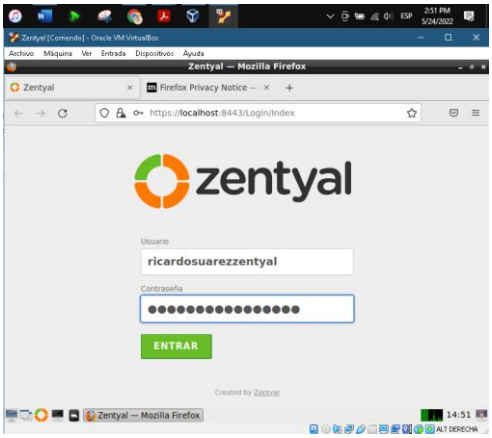

Figura 14. inicio de sesión

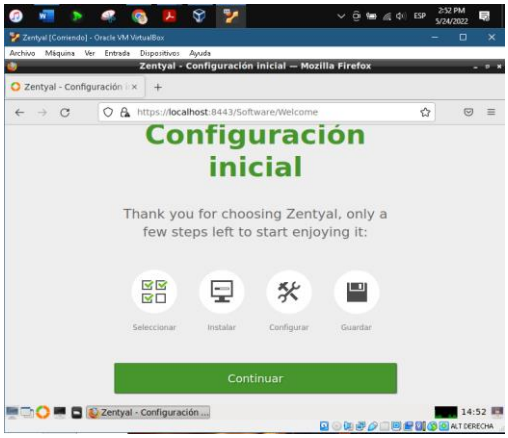

Figura 15. inicio de la configuración de Zentyal

3 DESARROLLO DE LAS TEMATICAS PROPUESTAS

3.1 TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

El servicio DHCP se utiliza para realizar una asignación IP dinámica en los equipos clientes y da la facilidad de estructurar una red de forma organizada y personalizada, como paso inicial con los adaptadores de red, como lo mencionamos anteriormente se debe habilitar 2 adaptadores, la primera que recibe la entrada del ISP y la segunda que funcionará como red interna para que los equipos clientes puedan leer unirse a la configuración y servicios instalados, una vez realizada esta configuración pasamos asignar la IP estática en el adaptador interno.

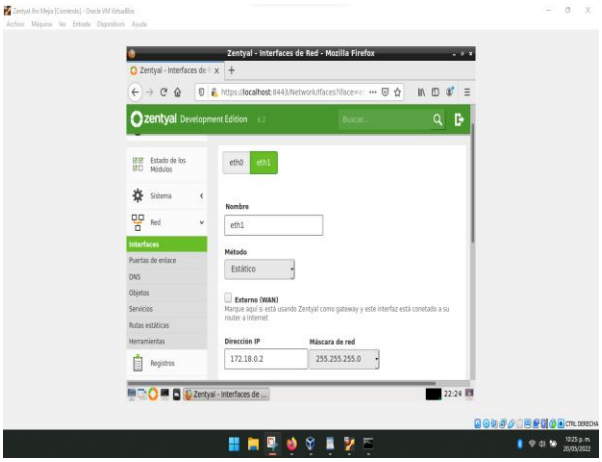

Figura 16. asignando IP

En la siguiente imagen del módulo DHCP arroja un broadcast referente a la IP estática configurada anteriormente, también se escoge unos rangos que serán asignados a los clientes en este caso elegir de 172.18.0.40 a 172.18.0.60.

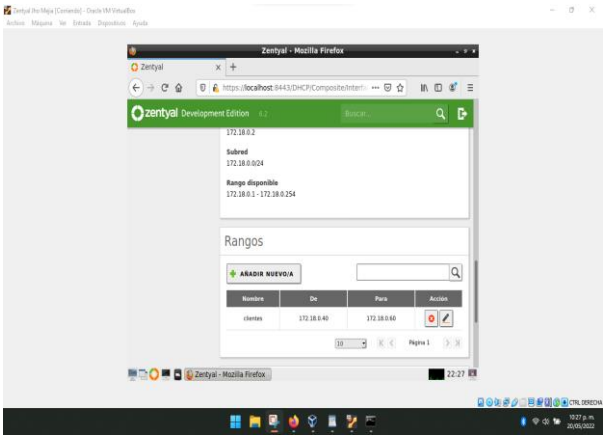

Figura 17. Rango IP DHCP.

Como paso a seguir se debe ir a nuestra máquina cliente Ubuntu Desktop y vamos a configurar el adaptador como red interna, sabiendo que esta red es la utilizada en el servidor Zentyal.

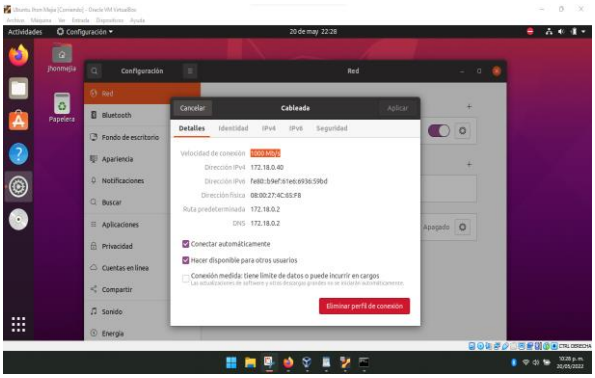
Figura 18. asignando IP

3.1.1 DOMINIO

Controlador de dominio o LDAP cumple con funciones de replicar información del directorio y clientes unidos al dominio aplicando políticas y parámetros que cumplas con requisitos asignados, ahora nos dirigimos a la pestaña de usuario y equipos, pueden crear los usuarios y grupos a los que van a asignar a los equipos clientes que serán unidos a el dominio.

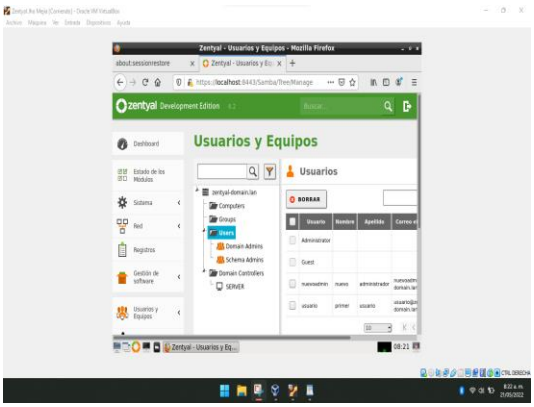

Figura 19. usuarios, grupos y equipos

Como primer paso ingresar un cliente Windows, siendo posible esta función debido a que Zentyal es compatible con este tipo de S.O, dirigirse a las propiedades de sistema, configuración avanzada y en la pestaña nombre de equipo ingresar el nombre del dominio al cual se desea realizar la unión y el nombre del equipo para identificarlo en el servidor.

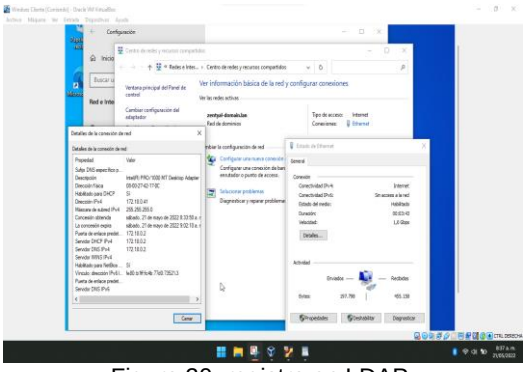

Figura 20. registro en LDAP.

Ahora para unir un cliente Ubuntu a el dominio en el servidor Zentyal, para obtener efectos y un resultado satisfactorio se descargar el siguiente paquete, dando el permiso para poder utilizar este paquete y con él ./ ejecutar la instalación.

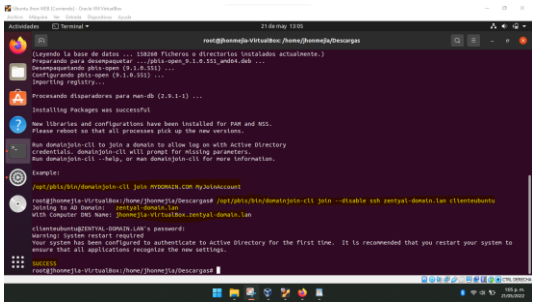

Figura 21. uniendo Ubuntu al LDAP.

Paso seguido ingresar usuario clienteubuntu, seguido del dominio @zentyal-domain.lan

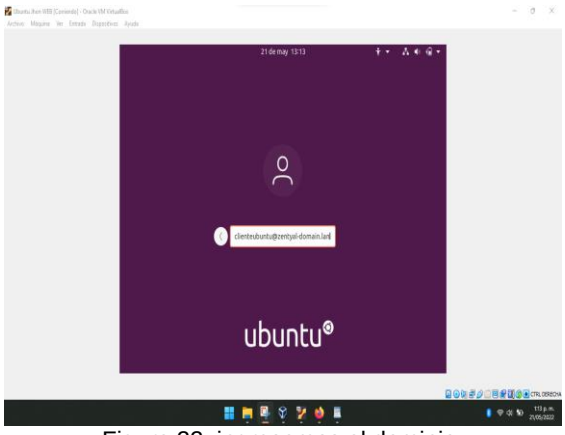

Figura 22. ingresamos al dominio.

Ahora se puede verificar en nuestro servidor zentyal que se haya unido el computador para finalizar todos los parámetros de configuración y comprobación de unión en el módulo LDAP.

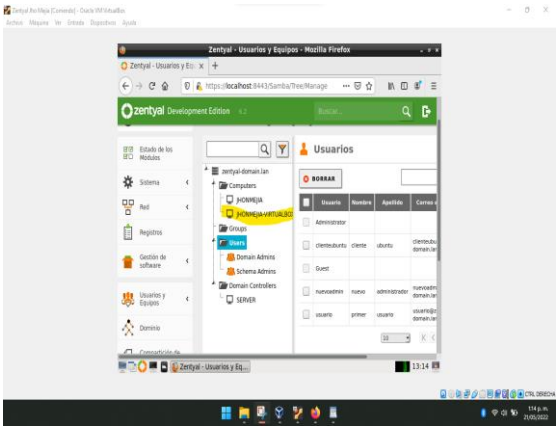

Figura 23. comprobamos registros.

3.1.2 DNS

En el módulo DNS pueden comprobar el nombre de dominio y parámetros de configuración para tener en cuenta para realizar ajustes.

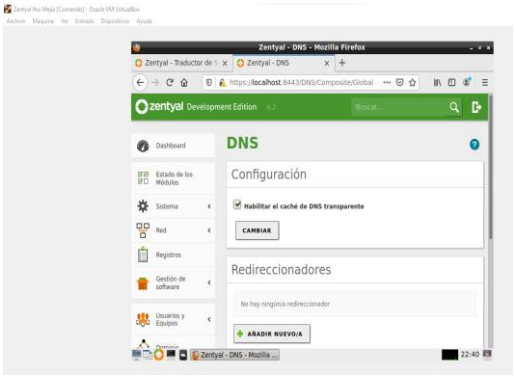

Figura 24. módulo DNS.

En el siguiente paso van a registrar los DNS de nuestro ISP y de Google, esto lo hacen para cuando los servidores por defecto no logren resolver algún nombre redireccione a otros servidores de dominios alternativos.

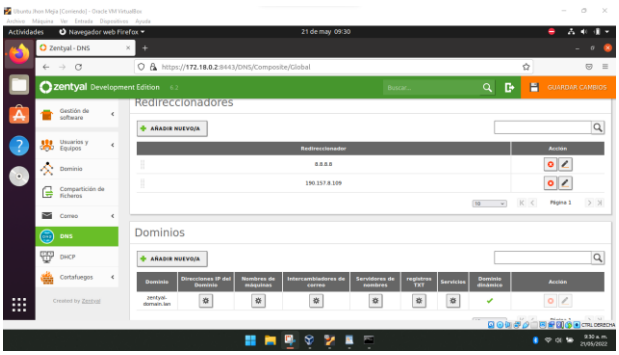

Figura 25. asignamos dns redireccionado.

En el siguiente procedimiento agregamos un DNS adicional que será utilizado para ser enrutado a un servidor WEB o que exista una instalación de algún CMS, el funcionamiento será nombrar o asignar un

nombre a cambio de poner la IP aunque también se puede realizar de esa forma.

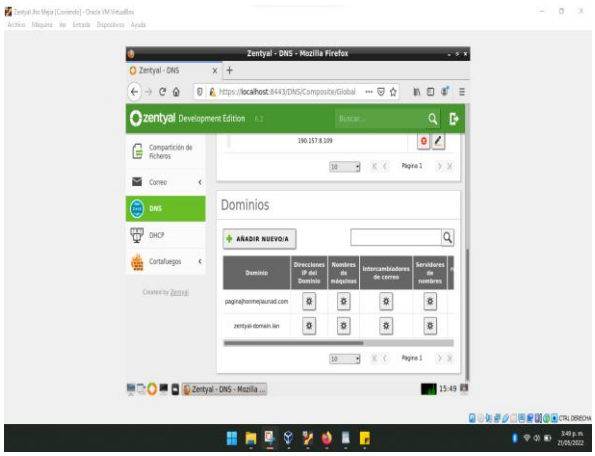

Figura 26. enrutando a un servidor web.

En la opción de la dirección IP se pone la del equipo o servidor al que se desea ingresar con el nombre de dominio y Finalmente se muestra que al digitar el nombre de dominio en el navegador ingresa a la IP del equipo en el servicio web.

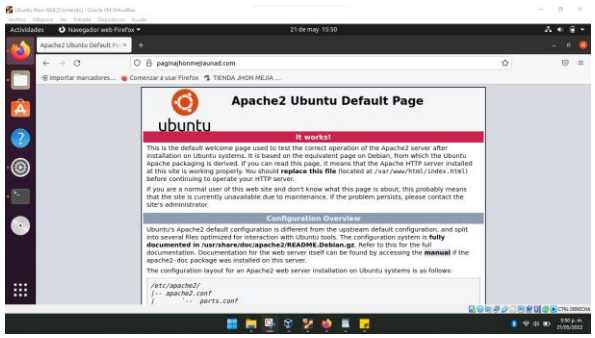

Figura 27. búsqueda por url.

3.2 TEMÁTICA 2: PROXY NO TRANSPARENTE

La implementación de un proxy ayuda a controlar el acceso a dominios o enlaces, tanto como permitir o denegar uno o muchos de estos. Debemos tener habilitado el módulo de HTTP Proxy para poder realizar este paso. Para implementar un proxy no transparente en Zentyal, vamos al apartado de red y objetos y creamos un objeto.

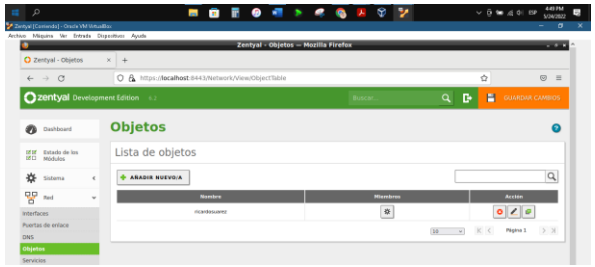

Figura 28. creación de objeto.

Una vez creado el objeto, ingresamos en las configuraciones de este y creamos un miembro, al cual le damos un nombre y dirección IP y canal.

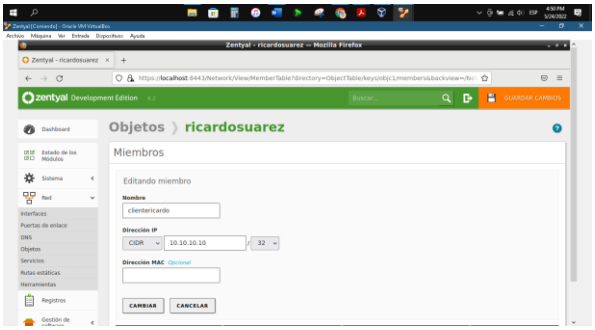

Figura 29. creación de miembro

Ingresar al apartado de red e interfaces y en eth1 cambiar la dirección IP por la deseada.

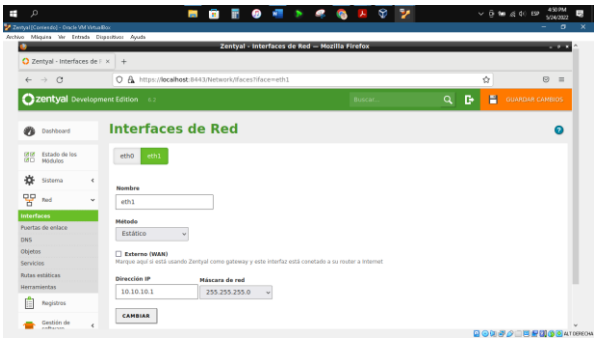

Figura 30. asignación de IP a la red interna

Ahora ir al apartado de Proxy HTTP-> perfiles y añadir un perfil.

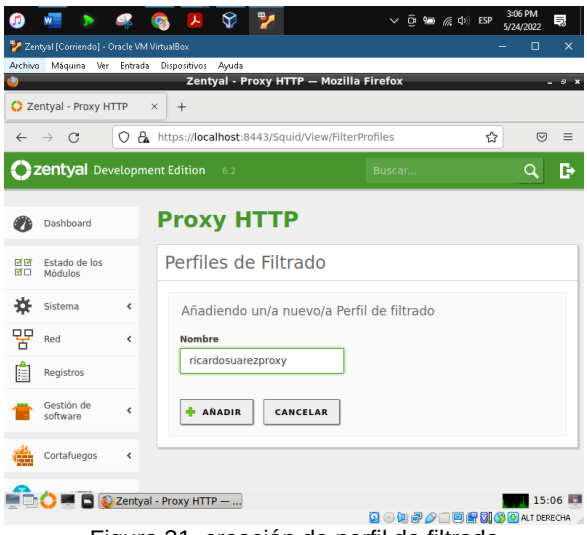

Figura 31. creación de perfil de filtrado

Ahora se entra a las configuraciones de este perfil, allí es donde se pueden crear reglas y excepciones de bloqueo para el proxy y vamos a reglas de dominios y URLs.

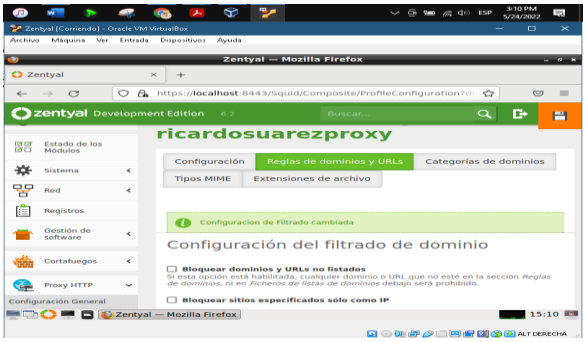

Figura 32. acceso a las reglas de dominios

Bajamos hasta reglas de dominios y se añade una regla, en este caso el dominio Facebook.com será denegado por el proxy.

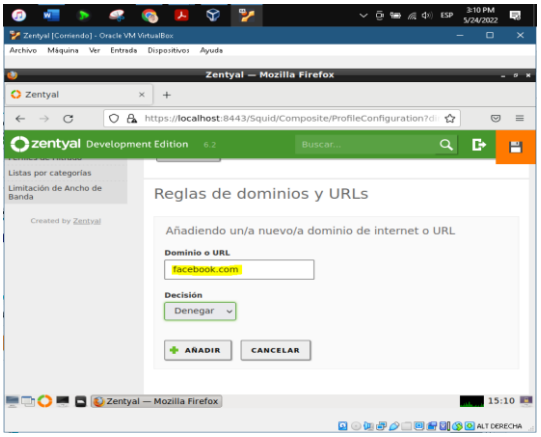

Figura 33. añadiendo reglas

Ahora vamos al apartado Proxy HTTP-> reglas de acceso y en la regla existente damos clic en editar.

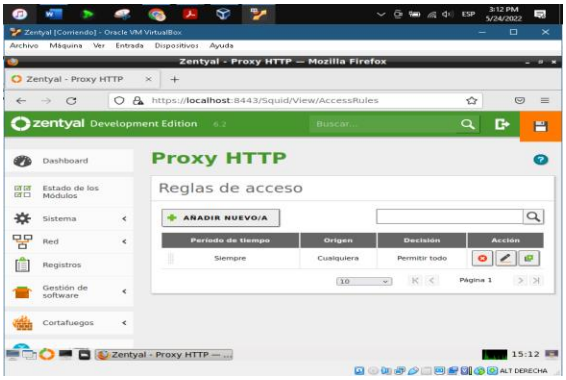

Figura 34. configurar las reglas de acceso

En el objeto de red elegimos el que creamos al inicio y en decisión aplicamos el perfil creado y damos en cambiar.

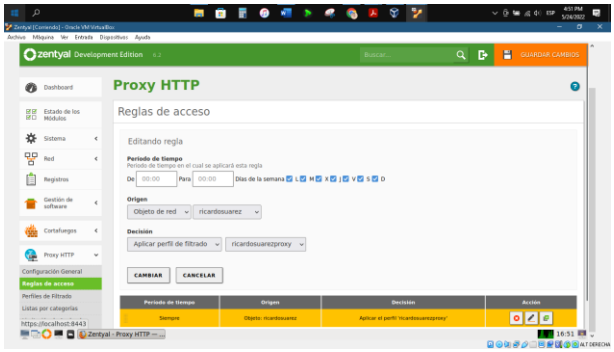

Figura 35. asignación de objeto y perfil a regla de acceso

Ahora vamos a la configuración general del Proxy HTTP y dejamos desmarcada la opción de proxy transparente, ya que lo queremos no transparente, y modificamos el puerto al 1320 que es el solicitado por la guía y damos clic en cambiar.

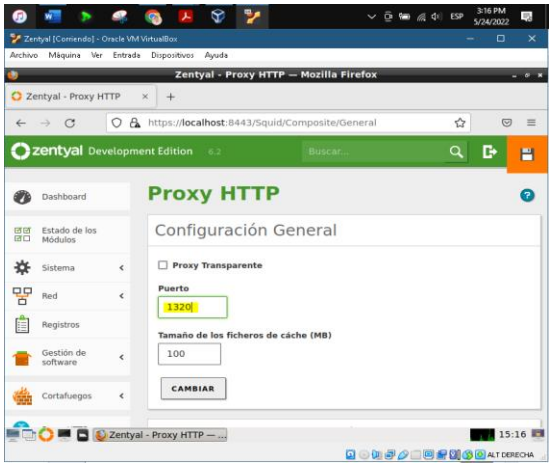

Figura 36. cambio de puerto al proxy

Se verifica en los estados de módulos que Proxy HTTP esté habilitado

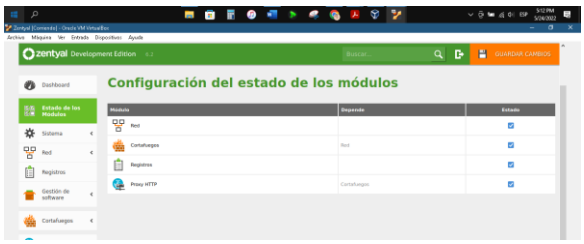

Figura 37. estado de los módulos

Una vez aquí se da clic en el icono de guardar en la esquina superior derecha del sistema y esperamos que los cambios se guarden. Si es necesario, vamos a la máquina cliente a configuraciones-> red y en la configuración de la conexión actual vamos a IPv4 y ponemos la conexión a Manual. Asignamos la dirección, máscara de red, puerta de enlace y servidores DNS. Esto para configurar el acceso al cliente de la red interna bajo la dirección y puerto proxy.

Por último, vamos a las configuraciones del navegador, a las configuraciones del proxy y lo

definimos manualmente como 10.10.10.1 y la puerta 1320.

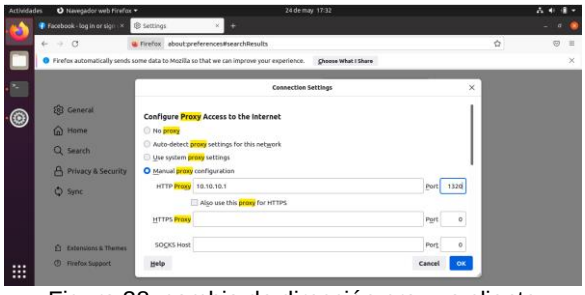

Figura 38. cambio de dirección proxy a cliente

Aquí ya podemos realizar una prueba de acceso al sitio y verificar que el acceso sea denegado, así como el acceso a cualquier otro sitio y que este siga normal.

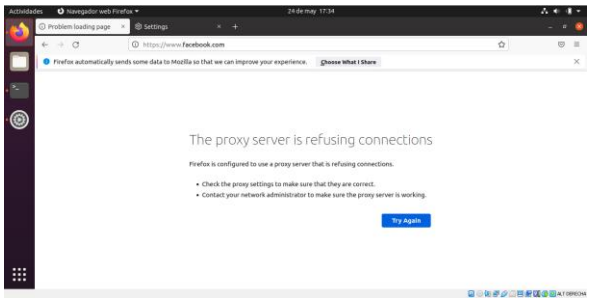

Figura 39. prueba de acceso denegado

3.3 TEMÁTICA 3: CORTAFUEGOS

Producto esperado: Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo.

El cortafuegos de Zentyal servirá como sistema de seguridad controlando el tráfico saliente y entrante no autorizado tanto del servidor como de la red interna, puede ser configurado con una amplia variedad de reglas ya sea para permitir, bloquear o filtrar datos y distintos tipos de peticiones.

De acuerdo con la temática selecciona se debe instalar los paquetes necesarios para configurar el módulo de Firewall y automáticamente se instalará el paquete de la configuración de la red

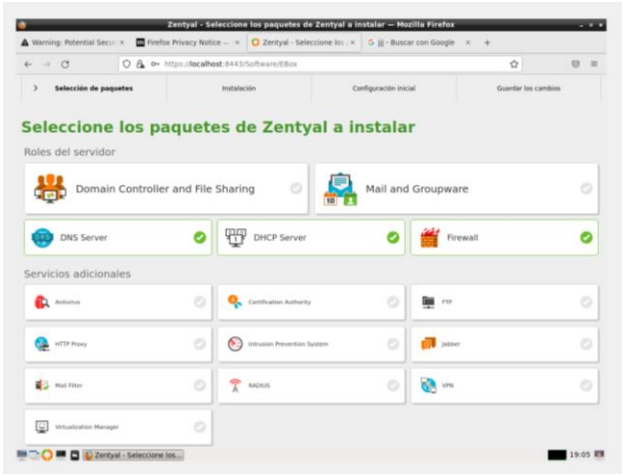

Figura 40. Paquetes de zentyal a instalar

Cuando Zentyal actúa como cortafuegos, normalmente se instala entre la red interna y el router conectado a Internet. Por tanto, la interfaz que se comunica con el router, debe ser marcada como externa (en este caso la eth0, que será la primera interfaz que contendrá la IP del router configurada como método estático

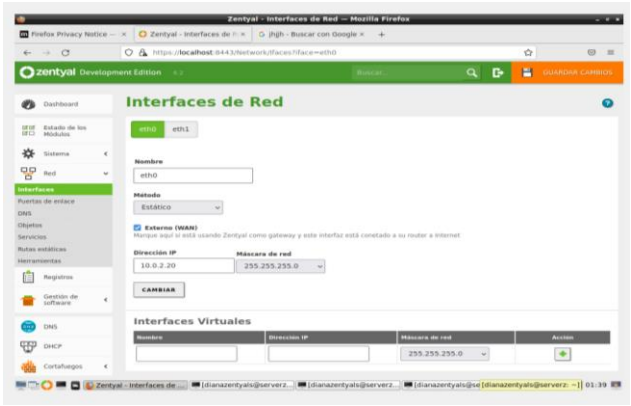

Figura 41. Configuración de red externa eth0

Luego se configura la puerta de enlace que proporcionara el acceso a internet, se selecciona puerta de enlace>Añadir Nuevo y se asigna un nombre y la dirección IP y dar en añadir y guardar cambios.

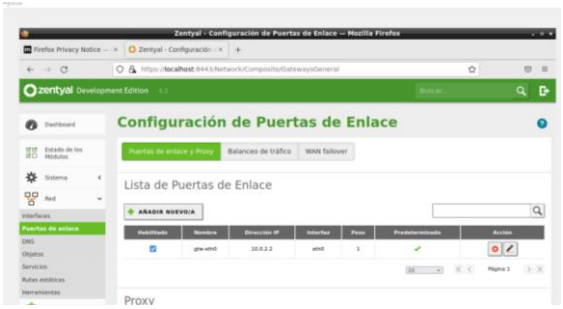

Figura 42. Puerta de enlace para la red eth0

En la segunda interfaz de red, La eth1 se configura como red interna, se asigna una dirección IP estática porque esta se utilizara como puerta de enlace para la

red local que que se debe asignar al equipo cliente (Ubuntu Desktop)

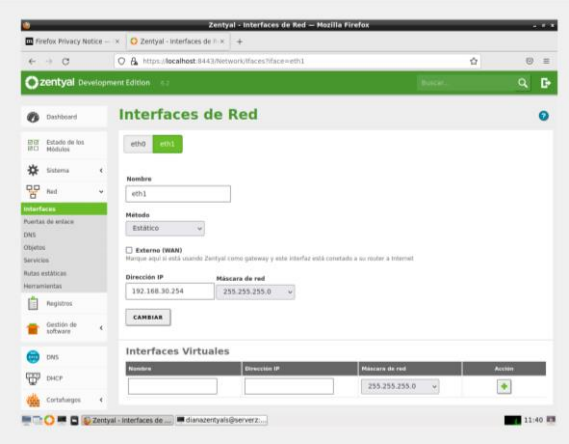

Figura 43. Configuración de red interna eth1

En la consola de Zentyal se ejecuta el comando ifconfig para confirmar que las IP se hayan asignado de forma correcta en las dos tarjetas eth0 y eth1

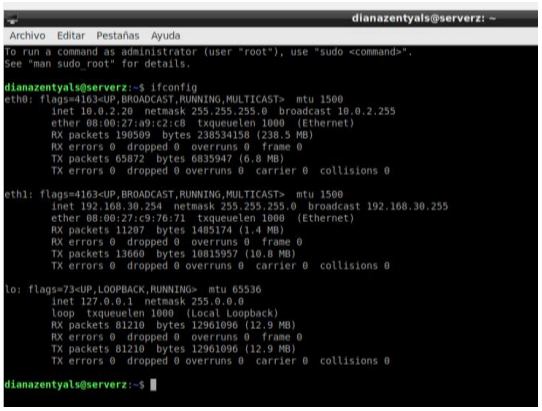

Figura 44. Zentyal ifconfig IP asignadas red eth0 y eth1

Se verifica que el servidor de zentyal tiene acceso a internet para luego configurar la máquina del cliente

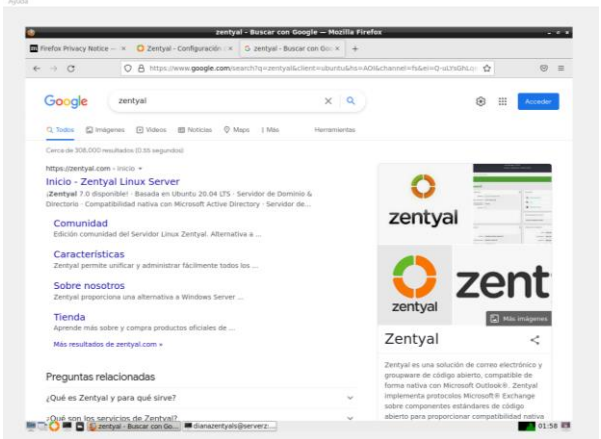

Figura 45. Servidor zentyal acceso a internet

Las interfaces de red en el servidor Zentyal que se le asignaron son: a la eth0 con adaptador NAT la IP 10.0.2.20 dentro de la zona DMZ y la eth1 con adaptador de red interna IP 192.168.30.254 dentro de la zona verde que se asignara al equipo con Ubuntu desktop

el esquema de red de las máquinas virtuales es el siguiente

Figura 46. Esquema de red máquinas virtuales

Se continúa configurando la interfaz de red del cliente con IP 192.168.20.110 que está dentro del rango de la red eth1.

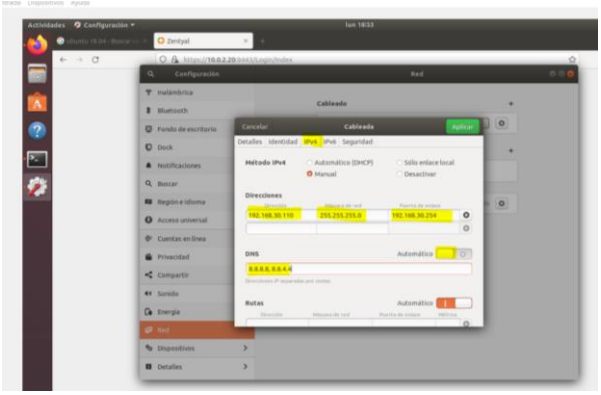

Figura 47. Configuración de red Ubuntu método estático

En la puerta de enlace (Gateway) se debe poner la misma IP de la interfaz eth1: 192.168.30.254 para poder proporcionar acceso a internet y en DNS se desactiva el modo automático y se pone 8.8.8.8 y 8.8.4.4 que son las direcciones IP de los servidores DNS públicos de Google y dar en aplicar.

Luego se abre la consola de Ubuntu para asignar los DNS. Para eso se edita el archivo /etc/resolv.conf con el comando nano, y se comenta el nameserver que aparecen allí, sino hacemos este paso no tendremos acceso a internet.

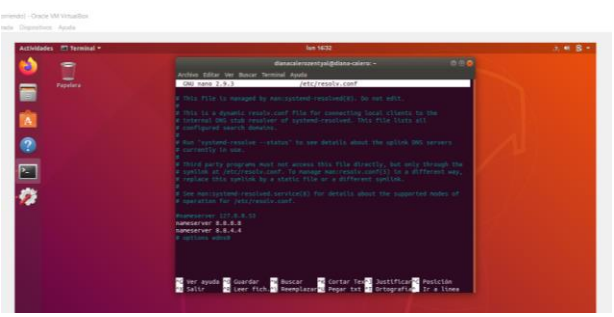

Figura 48. Definición de servidores de salida a internet

Se verifica por consola con el comando ifconfig la dirección IP que se asignó al equipo Ubuntu Desktop

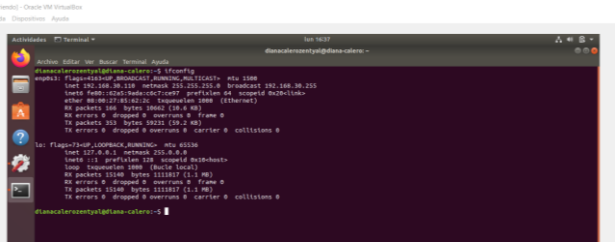

Figura 49. Verificación de IP Ubuntu desktop (cliente)

Se Verifica el acceso a internet de la maquina cliente.

Ahora se continua con la configuración de las **reglas de cortafuegos.** La definición de las políticas del cortafuegos se hace desde Cortafuegos ▸ Filtrado de paquetes.

Figura 50. Secciones del firewall, dependiendo del flujo de tráfico

Cada una de las secciones que se pueden ver en el diagrama controla diferentes flujos de tráfico, dependiendo del origen y destino:

Reglas de filtrado de redes internas a Zentyal
Reglas de filtrado para las redes internas
Reglas de filtrado desde las redes externas a Zentyal
Reglas de filtrado para el tráfico saliente de Zentyal

Antes de agregar las reglas se consulta la dirección IP de la web que se va a bloquear, en la terminal se ejecuta el comando nslookup seguido del dominio o también el comando ping seguido del nombre de dominio

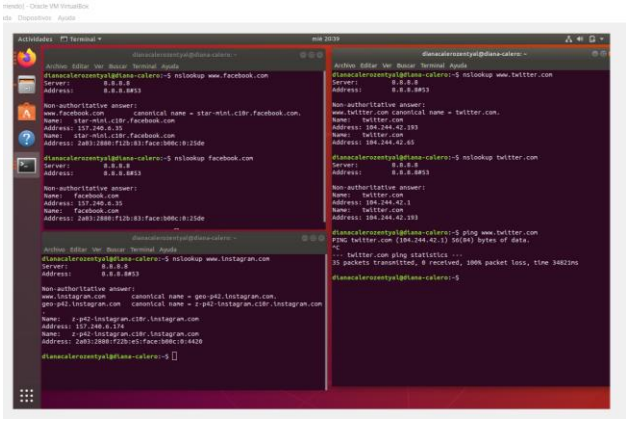

Figura 51. obtener IP de los sitios web por el dns de Google

Como se puede observar hay sitios que tienes dos direcciones IP, es decir que manejan un rango de IP, para contestar desde las diferentes direcciones.

Por tal motivo para crear las reglas de filtrado de paquetes se tendría que añadir una regla por cada IP que maneje para el mismo Sitio Web, por lo cual no es óptimo.

Para optimizar, con la IP obtenida, ir http://whois.arin.net/ui digitar en la parte superior derecha y obtener el rango de IP del sitio web

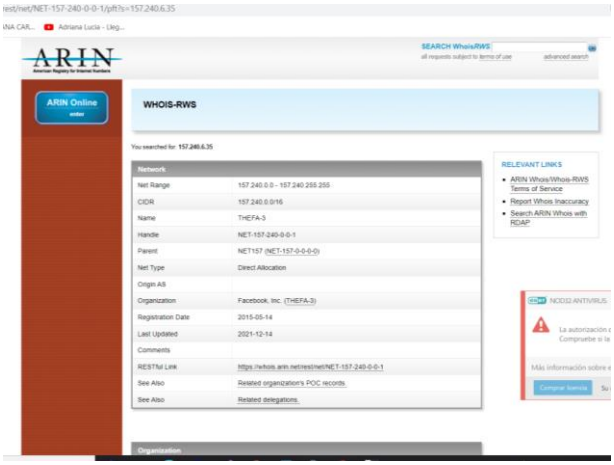

Figura 52. Arin consultar rangos de los sitios web a bloquear

Así mismo se consulta los rangos de IP para los demás sitios que se desea denegar el acceso. Luego se debe ir al apartado de Red>Objetos>Crear un objeto de red llamado ejemplo Facebook y dar en añadir

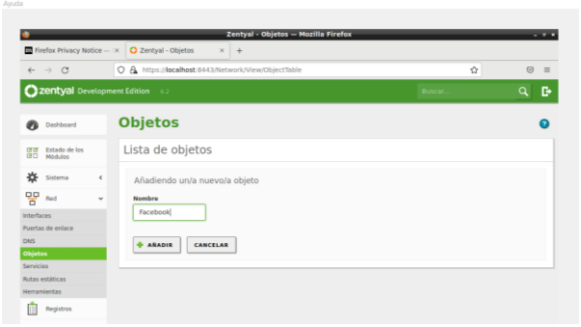

Figura 53. Crear objetos sitios web a bloquear

Se crean los demás objetos para Twitter e Instagram

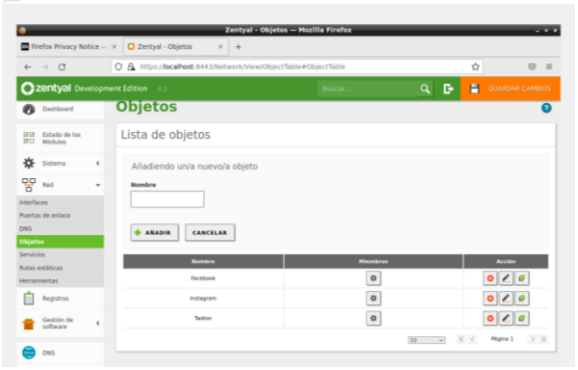

Figura 54. Lista de objetos creados

Se Continúa dando clic en el icono del engranaje para añadir un miembro por cada objeto, se le asigna el nombre que desee, en dirección IP escoger “rango” y colocar el rango respectivo que se consultó en whois, y dar en añadir.

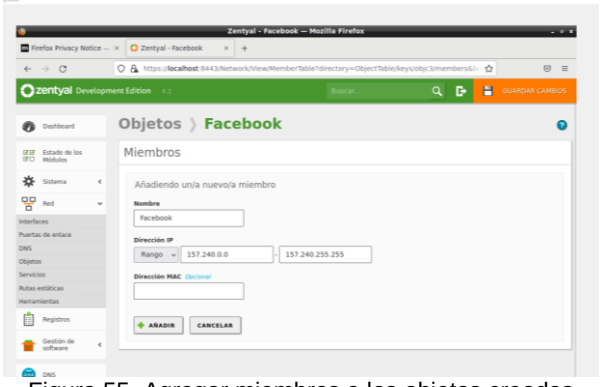

Figura 55. Agregar miembros a los objetos creados

Se realiza el mismo procedimiento para añadir los demás miembros a cada objeto creado

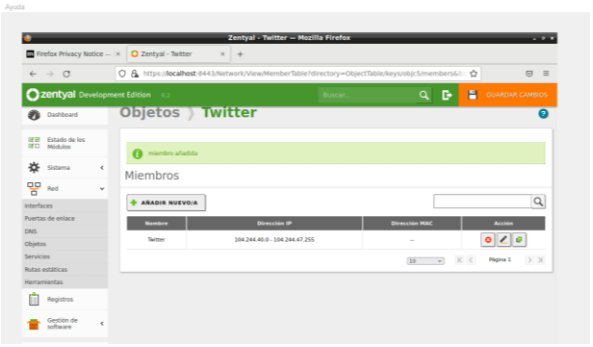

Figura 56. Lista de miembros asignado a Twitter

Luego se procede a bloquear el acceso a los objetos que se crearon con los rangos de Ip. Para crear las reglas se debe ir a *Firewall* > *Filtrado de paquetes* y escoger las reglas ***de filtrado para las redes internas*** y dar en configurar regla

Decisión: Denegar
Origen: 192.168.30.110/24 (red interna donde se encuentra el equipo con el Ubuntu
Destino: Objeto Destino Facebook
Servicio: Cualquiera

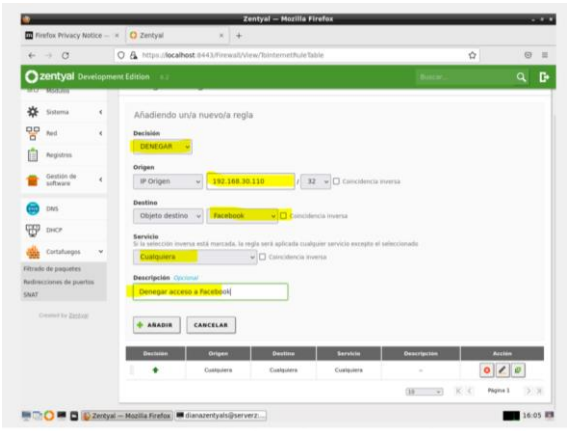

Figura 57. Crear reglas para redes internas

Así mismo se añaden las reglas para denegar el acceso a los objetos creados de Twitter e Instagram

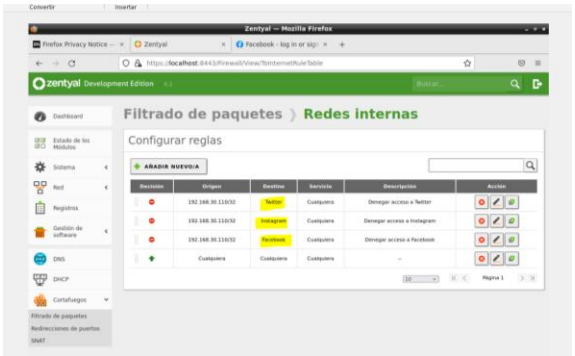

Figura 58. Lista de reglas para redes internas

Se verifica que el acceso es denegado a Facebook, Twitter e Instagram desde el equipo cliente Ubuntu, pero al mismo tiempo hay acceso a internet para otros sitios

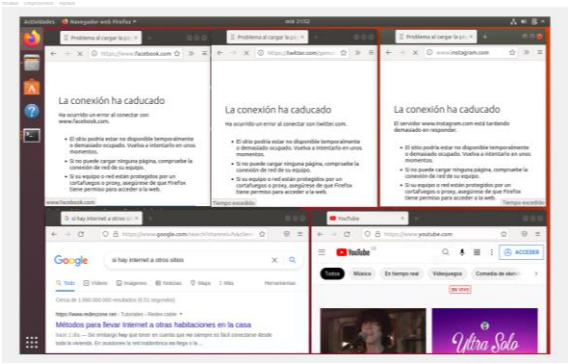

Figura 59. Comprobación de acceso a los sitios e internet

Se puede comprobar con el comando ping que no hay respuesta de envío de paquetes

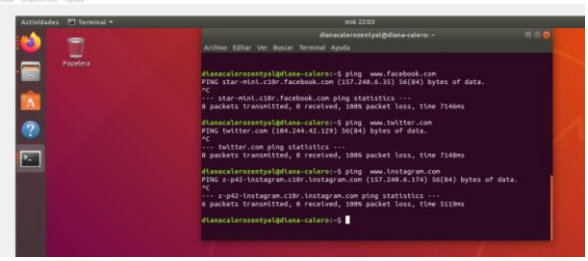

Figura 60. Ping sin comunicación a los sitios web

Aplicando las reglas, e intentando acceder desde la web a los diferentes sitios como Facebook, Twitter e Instagram y realizando comando ping no hay respuesta de envío de paquetes, entonces se ha configurado con éxito el cortafuego para el bloqueo de dichas páginas web.

3.4 TEMÁTICA 4: FILE SERVER Y PRINT SERVER

Complementos requeridos para la temática 4 File Server y Print Server.

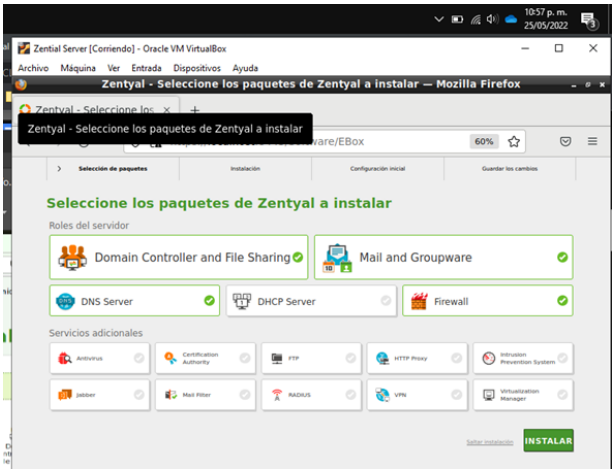

Figura 61. Instalación de complementos necesarios para la temática 4.

Ahora, se debe iniciar la configuración del servidor de archivos, tarea que se puede realizar sacando provecho de las herramientas previamente instaladas y de la capacidad del sistema operativo para la creación de permisos y perfiles de usuario por medio del paquete Samba para Linux. En la interfaz gráfica de zentyal se accede por el menú de usuarios y equipos.

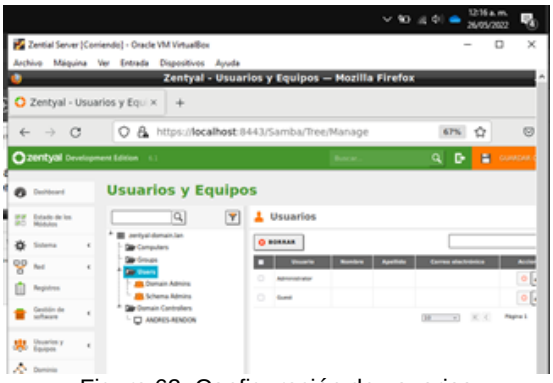

Figura 62. Configuración de usuarios

Crear la carpeta (diplomado).

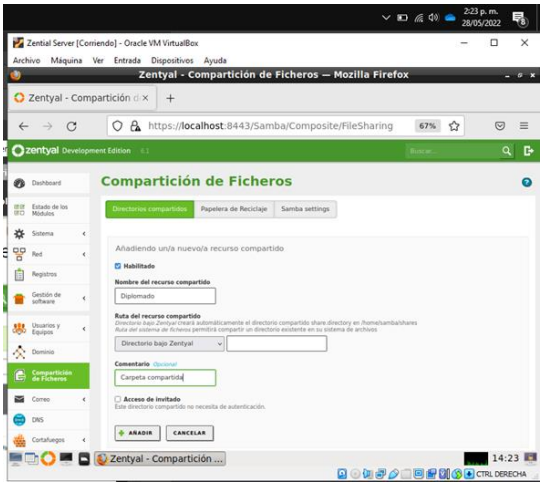

Figura 63. crear carpeta “diplomado”.

Se ingresa al Dashboard. Esto le crea el directorio compartido y se da clic en Añadir: hay que ingresar un nombre para la carpeta (diplomado).

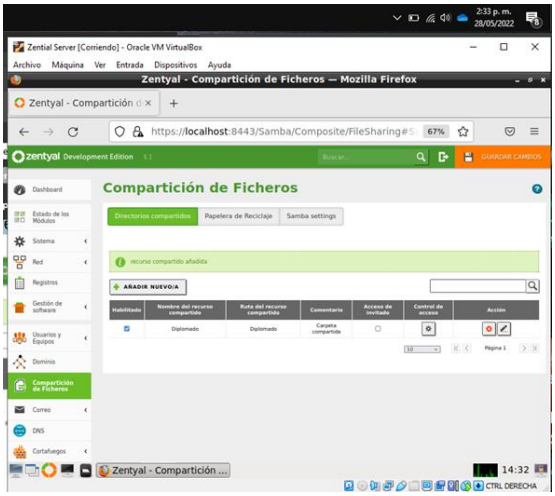

Figura 64. configuración carpeta “diplomado”.

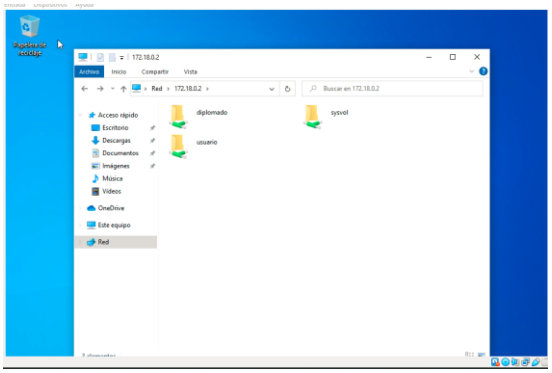

Figura 65. carpeta “diplomado”.

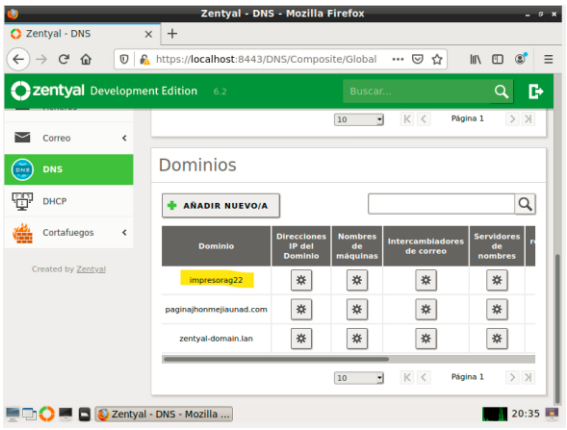

Figura 66. agregamos el DNS “impresoraG22”.

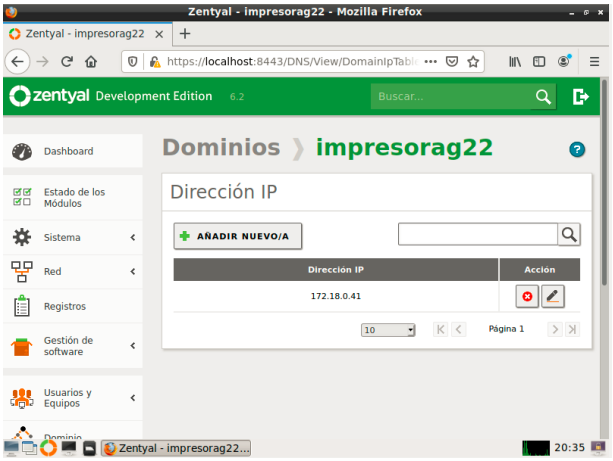

Figura 67. IP servidor Print

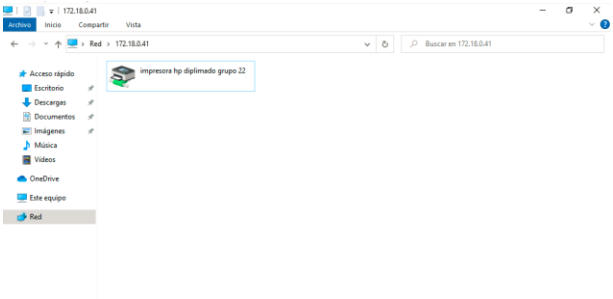

Figura 68. Ingreso desde Cliente

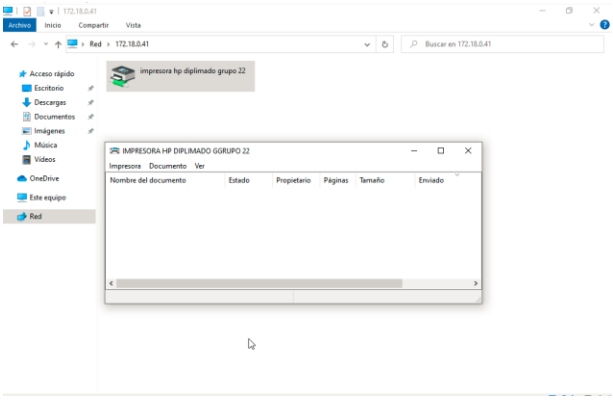

Figura 69. Instalación completa Impresora.

3.5 TEMÁTICA 5: VPN

Lo primero que se debe hacer para configurar una VPN es crear un certificado de la Autoridad de Certificación

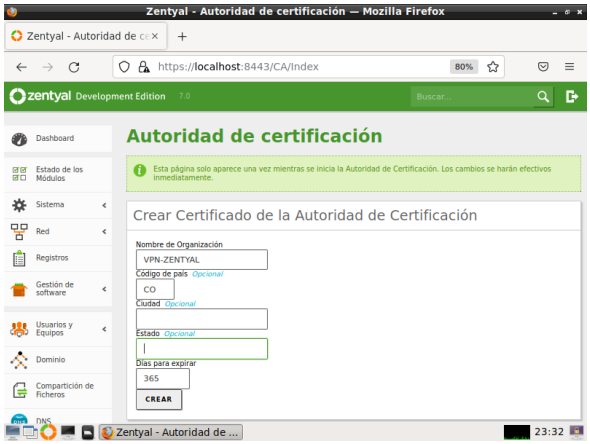

Figura 70. Crear certificado

Ahora se debe ingresar al módulo VPN → Servidores y agregar un servidor

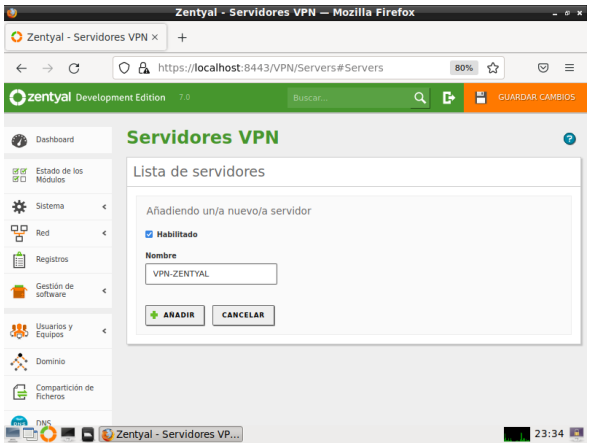

Figura 71. Agregar servidor

Con el servidor VPN creado, se procede a configurarlo

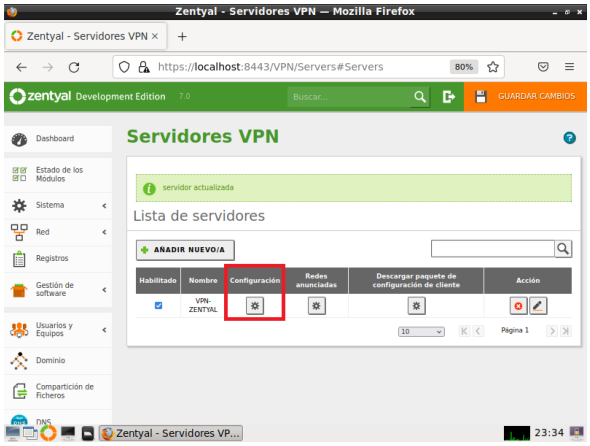

Figura 72. Configurar servidor

Para este caso se deja el puerto y la IP predeterminada que se genera

Figura 73. Puerto y dirección de red

Se habilita la interfaz TUN

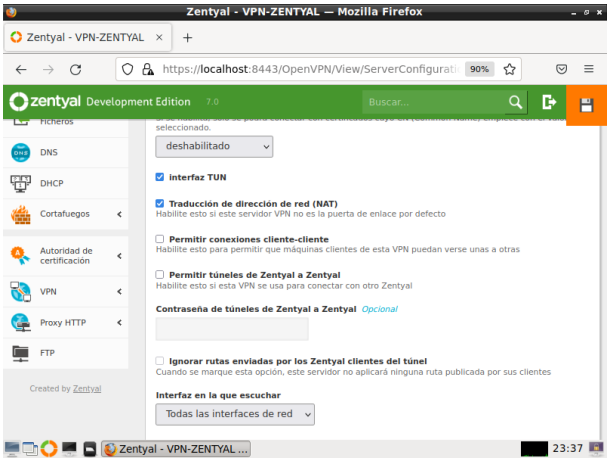

Figura 74. Interfaz TUN

También se habilita la opción “Redirigir puerta de enlace” para que sea el servidor quien entregue el internet, así la conexión se hace más segura

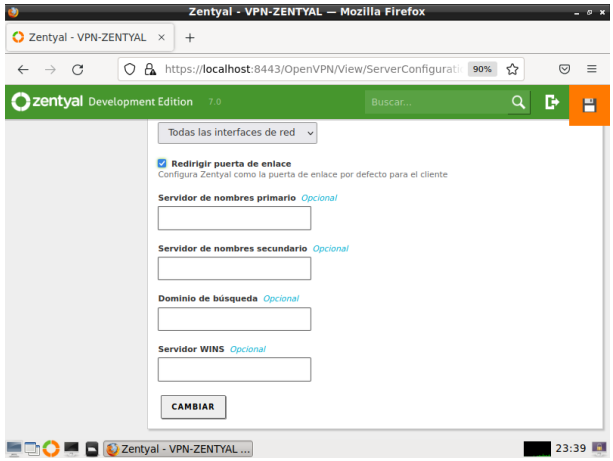

Figura 75. Redirigir puerta de enlace

Ahora hay que dirigirse a la sección “Servicios” y añadir un nuevo servicio el cual va a permitir la conexión al servidor

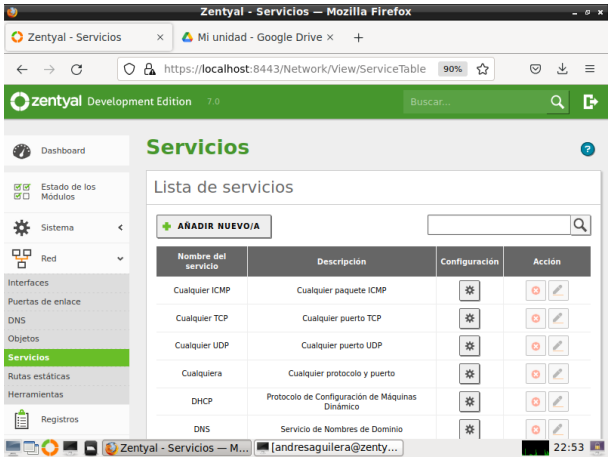

Figura 76. Añadir servicio

Se ingresa un nombre para el servicio y se agrega una descripción

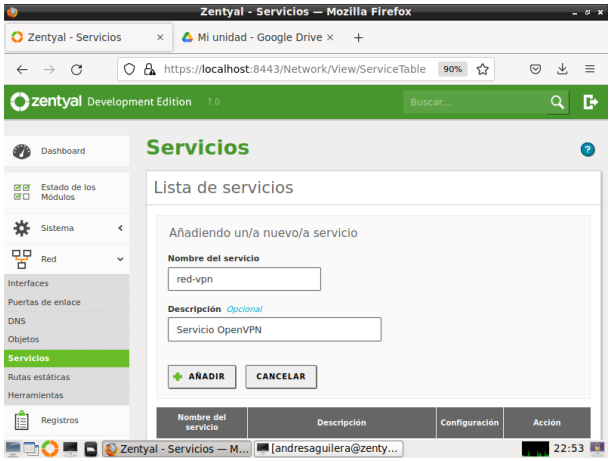

Figura 77. Nombre de servicio y descripción

Se procede a configurar el servicio que se ha creado anteriormente

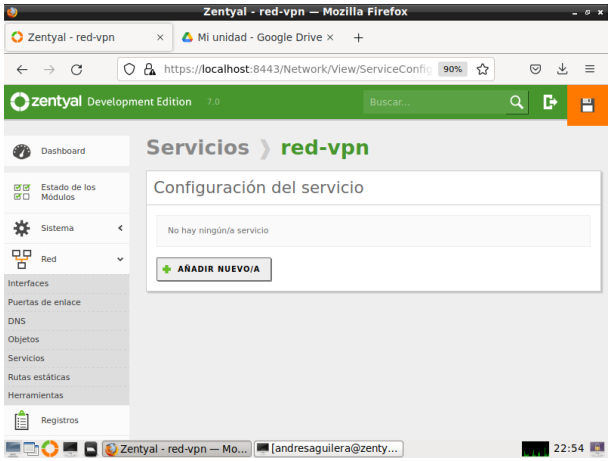

Figura 78. Configurar servicio

Seleccionar el protocolo UDP, en “Puerto destino” elegir “Puerto único” y agregar el puerto predeterminado el cual es 1194

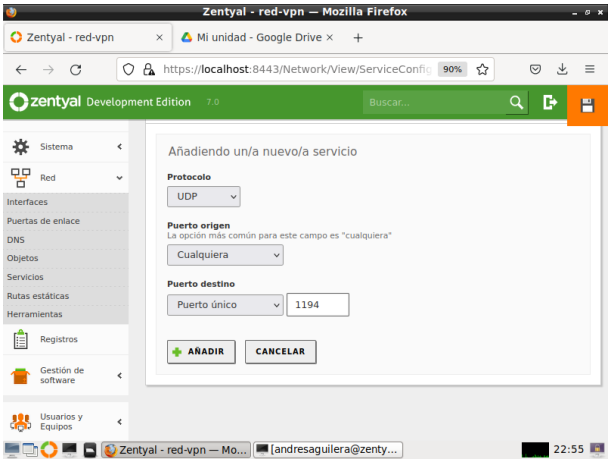

Figura 79. Protocolo y puerto de destino

Ahora hay que ingresar al módulo Cortafuegos → Filtrado de paquetes y configurar una regla para filtrado desde las redes internas a Zentyal

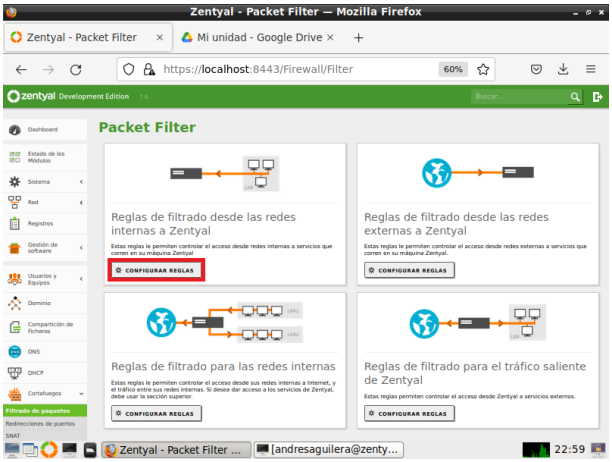

Figura 80. Configurar regla

Se añade una nueva regla en el cortafuegos

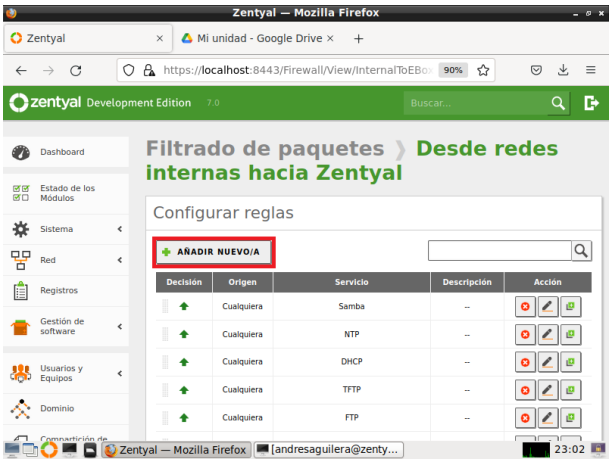

Figura 81. Añadir regla al cortafuegos

Elegir “ACEPTAR” para recibir conexiones desde cualquier origen. Así mismo, seleccionar el servicio que se creó previamente

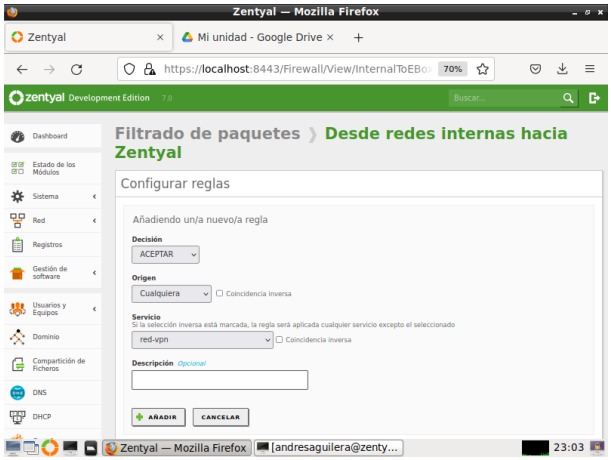

Figura 82. Configurar regla para el nuevo servicio

Se debe ingresar nuevamente al módulo VPN → Servidores y proceder a generar el paquete de configuración

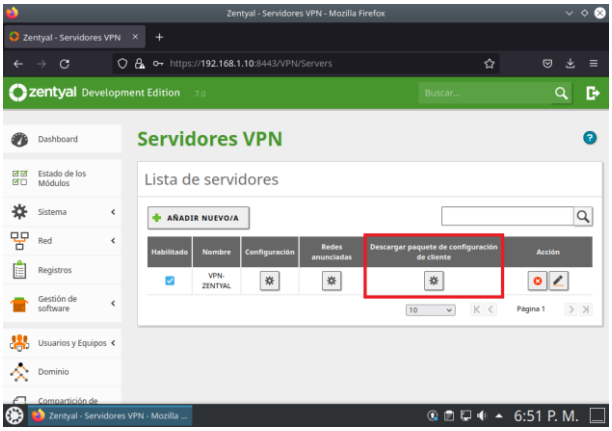

Figura 83. Generar paquete de configuración

En este ejemplo se elige generar el paquete de configuración para un cliente Windows, se ingresa la IP del servidor Zentyal y por último, se da clic en “DESCARGAR”

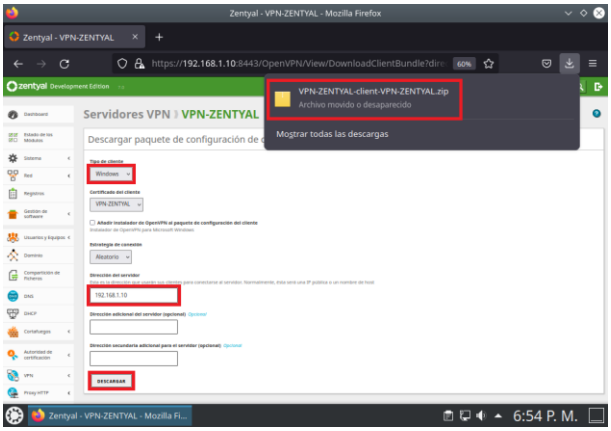

Figura 84. Descargar paquete para cliente Windows

Desde el equipo Windows, abrir la aplicación OpenVPN e importar el archivo de configuración que viene incluido en el paquete que se descargo

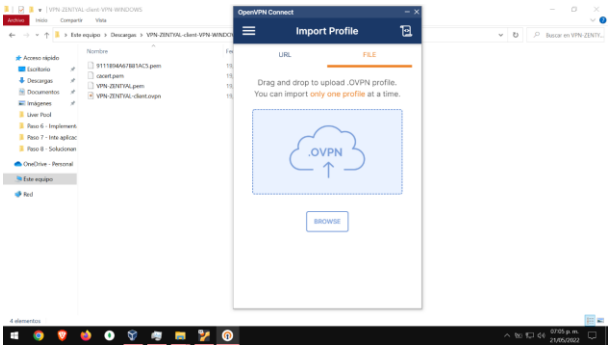

Figura 85. Abrir OpenVPN

Se procede a realizar la conexión y después de unos segundos se puede observar que se hizo satisfactoriamente

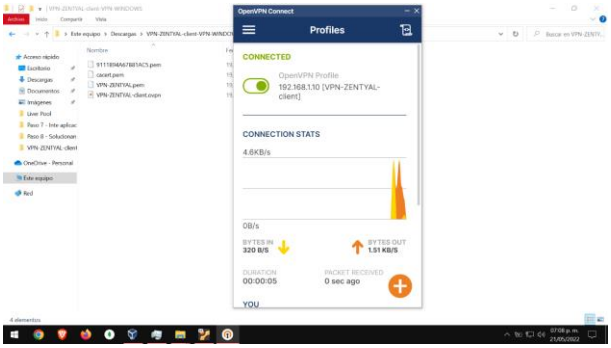

Figura 86. Conectar al servidor VPN

Como último paso, se procede a verificar la conexión ingresando por medio del navegador a una aplicación alojada en el servidor Ubuntu

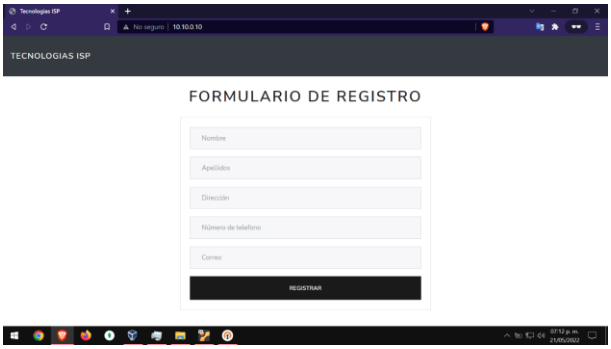

Figura 87. Verificar conexión

4 CONCLUSIONES

La importancia de implementar servicios y módulos que nos ayude a mejorar y brindar una alta calidad en infraestructura TI, el servidor Zentyal actúa como dispositivos ejecutando funciones como lo es firewall, DHCP, LDAP o controlador de dominio, DNS, Proxy, FTP y VPN entre otros, que ofrecen un valor para el control, gestión y seguridad en nuestra de red cumpliendo con el respaldo de los equipos clientes y servidores, así como restringir aplicaciones, bloquear puertos, direcciones y efectuar reglas que den salida o entrada a nuestro cliente bajo el suministro de nuestra red, para disminuir el riesgo de ataques, consumo de datos, restricciones manejo de cargas que ayuden al rendimiento para nuestra compañía.

El manejo de acceso con proxy ya sea transparente o no es simple para ser configurado y Zentyal tiene herramientas intuitivas para la configuración de este.

Se conoció sistema Zentyal como una alternativa para Active Directory de Windows para la administración de dominio y otras herramientas como las mencionadas al inicio.

A través de la práctica de Zentyal Server configurado para actuar como un cortafuegos dentro de una red perimetral y creando reglas para la restricción de acceso a sitios web de entretenimiento y redes sociales se evidencio que puede ser configurado con una amplia variedad de reglas ya sea para permitir, bloquear o filtrar datos y distintos tipos de peticiones. Además, es una alternativa en código abierto a Windows Server y Gracias a la interfaz gráfica se puede gestionar de forma sencilla un gran número de servicios, de esta manera impedimos que usuarios no autorizados accedan a nuestras redes privadas conectadas a internet. Podemos brindar mayor seguridad a nuestras redes locales de forma gratuita e intuitiva.

En conclusión, con esta actividad se evidencia la implementación y configuración de una herramienta que permite establecer conexiones remotas a través de túneles VPN, demostrando su correcto funcionamiento.

5 REFERENCIAS

[1] Documentación de Zentyal 6.2 (2018*). Configuración de un LDAP con Zentyal.* [En línea]. https://doc.zentyal.org/6.2/es/directory.html.

[2] Zentyal Community. (s. f.-b). *Servicio de Proxy HTTP — Documentación de Zentyal 6.2.* https://doc.zentyal.org/6.2/es/proxy.html.

[3] Documentación de Zentyal 6.2 (2018). *Configuración de un cortafuegos con Zentyal*. [En línea]. https://doc.zentyal.org/en/firewall.html.

[4] Zentyal para administradores de redes, (s.f), *Zentyal para administradores de redes, archivo* [PDF]. https://zentyal.com/wp-content/themes/storefront-zentyal-child/assets/files/sample_chapter_zentyal_vpn_openvpn_es.pdf

[5] Rodríguez, R. (2015, mayo 29*). Configuración y conexión a un servidor VPN con Zentyal usando OpenVPN*. Youtube. https://www.youtube.com/watch?v=3rNfipxE-9o.